AS Sertifitseerimiskeskus Sertifitseerimispõhimõtted – CPS

Versioon 2.4
OID: 1.3.6.1.4.1.10015.1.2.4
01.07.2009

Versiooni info		
Kuupäev	**Versioon**	**Muudatused**
30.04.2009	2.4	Uuendatud standardiviited RFC 2459 → RFC 3280 Keelelised korrektuurid Täiendused ja parandused: - Sissejuhatus - kaasajastatud asutajaliikmete nimed; - 1.1 - sertifitseerimispoliitikad edaspidi kooskõlastatakse SR-iga; - 1.2.3.2 – täiendatud digitaalse templi nõudega - 2.1.4 – sertifikaadi kehtivuse kontroll CRL vastu asendatud SK poolt pakutava kehtivusinfo abil - 2.1.5 – kataloogiteenus ei kajasta väljastatud sertifikaatide staatust - 2.1.5 – kustutatud: rakendatud peavad olema turvameetmed kataloogiteenuse teeskluse vältimiseks ja andmetervikluse tagamiseks - 2.4.1 – uuendatud avalikult kättesaadava informatsiooni asukohad, lisatud LDAP-i aadress; - 2.5 - kord poolaastas viiakse läbi sisemine audit siseaudiitori poolt; Auditi tulemused avaldatakse SK koduleheküljel. - 4.3.1 – kustutatud sertifikaatide kehtivuse peatamise ja kehtetuks tunnistamise kanalite hulgast avalik andmesidevõrk; - 4.4.1.4 – sertifikaadi omanikku teavitatakse sertifikaadi kehtivuse peatamisest kohe peale kehtivuse peatamistoimingu sooritamist - 4.5.4 - sertifikaadi omanikku teavitatakse sertifikaadi kehtivuse peatatuse lõpetamise toimingu edukast läbiviimisest koheselt 4.8 - SK kehtestab sisemised korrad, juhendid ja taasteplaanid kriisisituatsioonis tegutsemiseks, tagamaks teenuse osutamise turvalisus ja kvaliteet. 6.2.1 - SK kasutab pääsukontrollisüsteemi
07.10.2002	2.1	Lisatud turvaline logi (p.4.7.3)
01.02.2002	2.0	Muudetud eesmärgiga olla universaalseks alusdokumendiks erinevate sertifitseerimispoliitikate jaoks: - välja jäetud SK CA-de struktuur - CPS ei oma enam OID-i

		- ette nähtud võimalus osade protseduuride (nt isikusamasuse kontroll) lepingujärgseks delegeerimiseks - üldistatud on sertifikaatide ja CRL-ide profiilide punkte - ära jäetud palju ebaolulist ja/või ID-kaardi spetsiifilist Parandatud keelt ja vormindust, välja jäetud ebaolulist.
31.08.2001	1.1	Esmane versioon

Sisukord

1. Sissejuhatus

AS Sertifitseerimiskeskus (edaspidi SK) on asutatud 16 veebruaril 2001. a. Aktsiaseltsi omanikeks on võrdse 25%-suuruse osalusega AS Swedbank, AS SEB Pank, AS Elion Ettevõtted ja AS EMT. AS-i Sertifitseerimiskeskus põhitegevusalaks on digitaalallkirja kasutuselevõtuks vajalike sertifitseerimis- ja sellega seotud teiste teenuste osutamine, mis võimaldavad igapäevaelus turvalist ja tõendatud elektroonilist kommunikatsiooni nii riigiasutuste kui äriettevõtetega.

AS-i Sertifitseerimiskeskus missiooniks on kindlustada kliente usaldusväärse sertifitseerimisteenusega vastavalt Eesti Vabariigi õigusaktidele ja rahvusvahelistele standarditele, olla andmekaitse alal üks turvalisemaid asutusi Eestis ning kasutada tipptehnoloogiaid lähtudes konkreetsest vajadusest ja majanduslikust aspektist.

1.1. Ülevaade

Käesolev dokument (edaspidi CPS – *Certification Practice Statement*) kirjeldab AS-i Sertifitseerimiskeskus sertifitseerimispõhimõtteid ning sertifitseerimisteenuse osutamisel kasutatavaid protseduure.

Käesolevad sertifitseerimispõhimõtted laienevad ainult AS-i Sertifitseerimiskeskus tipmise sertifitseerija Juur-SK ja tema alamsertifitseerijate poolt väljastatud digitaalsetele sertifikaatidele.

Käesolev CPS on aluseks erinevate sertifitseerimispoliitikate koostamisel ja nendele vastavate sertifitseerimisteenuste pakkumisel AS-is Sertifitseerimiskeskus.

Käesolev CPS on registreeritud Sertifitseerimise Registris (edaspidi SR). Kõik käesoleva CPS-i alusel välja antud sertifitseerimispoliitikad, mis võimaldavad välja anda sertifikaate digitaalseks allkirjastamiseks digitaalallkirja seaduse (edaspidi DAS) [2] mõistes, kooskõlastakse SRR-iga.

Käesoleva CPS-i koostamisel on kasutatud IETFi (*Internet Engineering Task Force*) soovituslikku dokumenti RFC 2527 [7].

AS-i Sertifitseerimiskeskus tipmise sertifikaadi sertifitseerimispõhimõtete erilaienduses *Certificate Policies* viidatakse CPS-i versioonile 2.4 OID: 1.3.6.1.4.1.10015.1.2.4.

Käesolev CPS aitab saavutada AS-i Sertifitseerimiskeskus juhatuse poolt kinnitatud turvapoliitikas dokumenteeritud turvataset. Lähtuvalt AS-i Sertifitseerimiskeskus turvapoliitikast on andmeturve ning selle kõrgele tasemele toetuv usaldus turvalise ja kvaliteetse teenuse vastu AS Sertifitseerimiskeskuse ülim prioriteet.

1.2. Organisatsioon ja kasutusvaldkond

1.2.1. Sertifitseerimiskeskus (SK)

SK osutab sertifitseerimisteenust vastavalt käesoleva CPS-i põhjal koostatud sertifitseerimispoliitikale koos sellega seonduvate lisateenustega.

SK sertifitseerimisteenus hõlmab vaikimisi kogu võtmepaaride ja sertifikaatide elutsükliga seotud protseduure, mida on kirjeldatud käesolevas dokumendis. SK-l on õigus sõlmida lepinguid, millega delegeeritakse ülesandeid kolmandatele osapooltele. Delegeeritud ülesanded ja vastutuse jagunemine on kirjeldatud vastavas sertifitseerimispoliitikas.

Käesolev CPS on kõikide SK poolt hallatavate sertifitseerimisteenuste sertifitseerimispoliitikate baasdokumendiks. Vastava sertifitseerimisteenuse sertifitseerimispoliitika täpsustab siintoodud aluspõhimõtteid. Käesoleva CPS-i ja konkreetse sertifitseerimispoliitika vastuolu korral on sertifitseerimispoliitikas toodu ülimuslik.

Sertifitseerimispoliitika OID on toodud ära vastava sertifitseerija kinnitusvõtme sertifikaadi sertifitseerimispoliitika laienduses.

1.2.2. Registreerimiskeskus

1.2.2.1. SK klienditeeninduspunkt

SK klienditeeninduspunkt tegutseb SK esindajana SK ja Kliendi vahelistes suhetes. SK klienditeeninduspunkt, käesoleva CPS-i mõistes, võtab vastu avaldusi sertifikaatide taotlemiseks, uuendamiseks, kehtivuse lõpetamiseks, kehtivuse peatamiseks ja kehtivuse peatatuse lõpetamiseks.

SK klienditeeninduspunktide töötajad on saanud vastava koolituse kvaliteetse teenuse osutamiseks SK klientidele.

SK klienditeeninduspunktid ja nende arv võivad erinevate sertifitseerimispoliitikate puhul olla erinevad. SK klienditeeninduspunkti ja SK vaheline suhe on ära määratud kahepoolse(te) lepingu(te)ga.

Informatsiooni SK klienditeeninduspunktide ja nende kontaktandmete kohta esitatakse SK koduleheküljel vastava avaliku teenuse dokumentatsiooni juures.

1.2.2.2. Abiliin

Abiliin tegeleb SK esindajana klientide telefoniteenindusega ja võtab ööpäevaringselt klientidelt ja teistelt osapooltelt vastu taotlusi sertifikaatide kehtivuse peatamiseks, eelnevalt kontrollides isikusamasuse vastavalt sertifitseerimispoliitikas määratud isikusamasuse kontrolli protseduuridele.

Informatsiooni abiliini ja tema kontaktandmete kohta esitatakse SK koduleheküljel. Samas on toodud ära ka juhised abiliini poole pöördumiseks.

1.2.3. Kasutaja

1.2.3.1. Klient

Klient on käesoleva CPS-i alusel koostatud sertifitseerimispoliitika alusel väljastatud sertifikaadi omanik.

Kliendi eraldusnimi sertifikaadis koostatakse vastavalt sertifitseerimispoliitikates toodud sertifikaadiprofiilile, mis on koostatud vastavalt punktis 7.1 toodud nõuetele. SK tagab kliendi eraldusnime (*distinguished name*) ja sertifitseerija kinnitusvõtme sertifikaadi eraldusnime (*issuer name*) kombinatsiooni unikaalsuse.

1.2.3.2. Huvitatud isik

Huvitatud isik on osapool, kes võtab vastu otsuse kasutades selleks ka SK poolt väljastatud sertifikaati.

Huvitatud isik:

- arvestab põhimõtetega, mis on toodud konkreetse sertifikaadi sertifitseerimispoliitikas, käesolevas CPS-is ja nendes viidatud dokumentides;
- kontrollib sertifikaadi kehtivust SK poolt pakutava kehtivusinfo abil;
- kontrollib sertifikaadi kasutusala vastavust;
- kontrollib digitaalset allkirjastamist või digitaalse templi kasutamist võimaldavate sertifikaatide puhul digitaalselt allkirjastatud või tembeldatud andmekogumi terviklikkust ja identifitseerib allkirjastaja;
- lähtub digitaalallkirja või digitaalse templi kontrollimisel sertifikaadi kehtivusest digitaalallkirja või digitaalse templi andmise hetkel.

1.2.4. Sertifikaatide kasutusvaldkond

Sertifikaatide kasutamine peab olema kooskõlas sertifikaadi sertifitseerimispoliitikas toodud nõuete ja Eesti Vabariigi kehtestatud õigusaktidega.

Väljastatavate sertifikaatide kasutusvaldkond võib vastavalt sertifikaadiprofiilile olla piiratud. Vastavad piirangumehhanismid on kirjeldatud sertifikaadi väljastamisel aluseks olevas sertifitseerimispoliitikas.

Sertifitseerimispoliitikas ja sellega kaasnevas sertifikaatide profiilis määratakse ära, kas vastavaid sertifikaate saab kasutada digitaalallkirja seaduse mõttes. Käesolev CPS ei sea mingeid piiranguid selliste sertifitseerimispoliitikate koostamisele ning toetub oma põhimõtetes täie vastavusega digitaalallkirja seadusele.

Käesolev CPS ei piira SK poolt väljastatud sertifikaatide kasutamist erinevates tarkvararakendustes.

1.3. Kontaktandmed

Kõikides sertifitseerimisteenusega, sh sertifitseerimiskeskuse, registreerimiskeskuse ja abiliini tegevusega seotud küsimustes tuleb pöörduda järgnevalt toodud aadressil:

AS Sertifitseerimiskeskus
Äriregistri kood 10747013
Pärnu mnt 12, 10148 Tallinn
Tel +372 610 1880
Faks +372 610 1881
E-post: pki@sk.ee
http://www.sk.ee/

Kontaktandmete muutumisel teavitatakse sellest koheselt SK koduleheküljel.

2. Üldtingimused

2.1. Kohustused

2.1.1. Nõuded SK-le

SK tagab, et:

- sertifitseerimisteenuse osutamine on kooskõlas digitaalallkirja seaduse ja sellega seonduvate normatiivaktidega;
- sertifitseerimisteenuse osutamine on kooskõlas käesoleva CPS-iga.

SK kohustub:

- avalikustama oma sertifitseerimispõhimõtted ja sertifikaatide sertifitseerimispoliitikad ning tagama nende kättesaadavuse üldkasutatavas andmesidevõrgus;
- tagama sertifitseerimisteenuse osutamisel teatavaks saanud avaldamisele mittekuuluva teabe saladuses hoidmise;
- pidama arvestust enda poolt väljastatud sertifikaatide ja nende kehtivuse üle;
- võtma digitaalallkirja võimaldavate sertifikaatide puhul vastu ööpäevaringselt avaldusi sertifikaatide kehtivuse peatamiseks;
- tõendama digitaalallkirja võimaldavate sertifikaatide puhul huvitatud isiku nõudel oma esindaja digitaalallkirjaga enda poolt väljastatud sertifikaadis sisalduva avaliku võtme kehtivust;
- tagama ööpäevaringselt sertifikaatide kehtivuse kontrollivõimaluse üldkasutatavas andmesidevõrgus;
- säilitama sertifitseerimisega seotud dokumentatsiooni oma tegevuse lõpuni;
- tagama igal aastal infosüsteemi auditi teostamise ning esitama auditi tulemused sertifitseerimisteenuse osutajate riikliku registri volitatud töötlejale, et tagada enda püsiv registreeritus Sertifitseerimise Riiklikus Registris;
- avalikustama kohustusliku kindlustuslepingu tingimused üldkasutatavas andmesidevõrgus.

SK töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.2. Nõuded registreerimiskeskusele

2.1.2.1. Nõuded klienditeeninduspunktile

Klienditeeninduspunkt peab vastu võtma taotlusi sertifikaatide väljastamiseks, kehtivuse peatamiseks, kehtivuse peatatuse lõpetamiseks ja kehtetuks tunnistamiseks ning kontrollima nende avalduste õigsust ja terviklikkust. Klienditeeninduspunkt kohustub kõikide nimetatud toimingute teostamisel kontrollima taotluse esitaja isikusamasust ja volitusi toimingu teostamiseks.

Klienditeeninduspunkt peab edastama õiged ja terviklikud andmed SK-le.

Klienditeeninduspunkti peab teenuse osutamist takistava tehnilise rikke korral teatama sellest koheselt SK-le ja tegema kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

Klienditeeninduspunkt garanteerib oma töötajatele teenuse kvaliteetseks osutamiseks vajaliku koolituse.

Klienditeeninduspunkti töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.2.2. Nõuded abiliinile

Abiliin peab vastama Kliendi kõnele ööpäevaringselt 7 päeva nädalas.

Abiliin peab teenuse osutamist takistava tehnilise rikke korral teatama sellest koheselt SK-le ja tegema kõik endast oleneva võimaliku rikke likvideerimiseks esimesel võimalusel.

Abiliini töötajal ei tohi olla karistatust tahtlikult toimepandud kuriteo eest.

2.1.3. Nõuded kliendile

Klient peab järgima SK poolt käesolevas CPS-is kehtestatud nõudeid.

Klient peab sertifikaaditaotluses esitama õiget ja piisavat informatsiooni ning sertifikaati kantud andmete muutumise korral teatama õiged andmed vastavalt sertifikaadi sertifitseerimispoliitikas kehtestatud reeglitele. Klient peab olema teadlik sellest, et SK võib keelduda sertifikaadi väljastamisest, kui Klient on sertifikaaditaotluses teadlikult esitanud valeinformatsiooni või informatsiooni, mis on ebakorrektne või mittetäielik.

Klient peab oma isiklikke võtmeid ja neile vastavaid sertifikaate kasutama SK poolt ettenähtud korras ja viisil.

Klient peab teatama isikliku võtme tema nõusolekuta kasutamise võimalusest viivitamatult SK-le ning peatama sertifikaadi kehtivuse või tunnistama kehtetuks oma sertifikaadi.

Klient vastutab ainuisikuliselt oma isikliku võtme hoidmise eest. Klient peab isikliku võtme kasutamisel lähtuma käesoleva CPS-i punktis 6.1.2.3 toodust.

Klient peab olema teadlik, et DAS-i mõttes on aegunud, kehtetuks tunnistatud või peatatud kehtivusega digitaalallkirja sertifikaadi alusel antud digitaalallkirjad kehtetud.

2.1.4. Nõuded huvitatud isikule

Huvitatud isik peab tutvuma sertifikaadi aktsepteerimisega seotud kohustuste ja riskidega, mis on toodud käesolevas CPS-is ja konkreetse sertifikaadi sertifitseerimispoliitikas.

Kui sertifikaadiga või digitaalallkirjaga ei kaasne piisavalt tõendusmaterjali sertifikaadi kehtivuse kohta, peab huvitatud isik kontrollima sertifikaadi kehtivust sertifikaadi kasutamise või digitaalallkirja andmise ajal SK poolt pakutava kehtivusinfo abil.

Huvitatud isik peab jälgima sertifikaati kantud piiranguid ning veenduma aktsepteeritava tehingu spetsiifika vastavuses sertifitseerimispoliitikaga.

2.1.5. Nõuded kataloogiteenusele

Kataloogiteenuse eesmärgiks on võimaldada klientidele, huvitatud isikutele jt osapooltele juurdepääs sertifikaadiregistrile, et pärida informatsiooni sertifikaatide ning nende kehtivuse kohta.

Täpsed nõuded kataloogiteenusele tuuakse ära sertifitseerimispoliitikas.

Kataloogiteenus peab vastama järgmistele nõuetele:

- kataloog peab sisaldama väljastatud aegumata sertifikaate.
- kataloog ei tohi sisaldada delikaatseid isikuandmeid isikuandmete kaitse seaduse [5] mõistes;
- kataloog peab olema ööpäevaringselt kättesaadav avalikus andmesidevõrgus

2.2. Vastutus

2.2.1. SK vastutus

SK vastutab kõigi punktis 2.1.1 ja 2.1.5 toodud kohustuste täitmise eest Eesti Vabariigis kehtivates õigusaktides nõutud piirides.

2.2.2. Registreerimiskeskuse vastutus

2.2.2.1. Klienditeeninduspunkti vastutus

Klienditeeninduspunkt vastutab kõigi punktis 2.1.2.1 toodud kohustuste täitmise eest.

2.2.2.2. Abiliini vastutus

Abiliin vastutab kõigi punktis 2.1.2.2 toodud kohustuste täitmise eest.

2.2.3. Vastutuse piirid

SK ei vastuta klientide isiklike võtmete salastatuse, sertifikaatide võimaliku väärkasutuse ning huvitatud osapoole poolse sertifikaatide puuduliku kontrolli eest.

SK ei vastuta enda kohustuste mittetäitmise eest, kui selle põhjuseks on sertifitseerimise riikliku registri, andmekaitse järelevalveasutuse või mistahes muu avalik-õigusliku asutuse poolsed vead või turbeprobleemid.

Sertifitseerimispõhimõtetest tulenevate kohustuste mittetäitmist ei loeta rikkumiseks, kui selle põhjuseks on kohustuse täitja kontrollile mittealluv nn vääramatu jõud (*Force Majeure*).

2.3. Vaidluste lahendamine

Kõik osapooltevahelised vaidlused lahendatakse läbirääkimiste teel. Kokkuleppe mittesaavutamise või kestvate eriarvamuste korral lahendatakse vaidlused SK asukohajärgses kohtus.

Pretensioonist tuleb teisi osapooli teavitada hiljemalt 30 kalendripäeva jooksul pretensiooni põhjuse ilmnemisest, kui õigusaktides ei ole sätestatud teisiti.

2.4. Informatsiooni avaldamine ja kataloogiteenus

2.4.1. SK informatsiooni avaldamine

SK kehtiv juursertifikaat ning juursertifikaatide arhiiv avaldatakse aadressil http://www.sk.ee/certs.

Kõik otseselt sertifitseerimistegevusega seotud SK dokumendid on kättesaadavad avalikus andmesidevõrgus aadressilt https://www.sk.ee/repository.

Tühistusnimekirju avaldatakse aadressil http://www.sk.ee/crls.

Väljastatud sertifikaate avaldatakse sertifitseerimispoliitikas toodud korra kohaselt aadressil ldap://ldap.sk.ee.

SK tagab kogu eelpool nimetatud informatsiooni tervikluse ja kättesaadavuse ööpäevaringselt 7 päeva nädalas.

2.4.2. Avaldamise sagedus

Maksimaalne lubatud viivitus sertifikaadi staatuse muutumise registreerimisest uue tühistusnimekirja väljastamiseni ning tühistusnimekirja kehtivusaeg sätestatakse vastavas sertifitseerimispoliitikas.

SK tagab oma koduleheküljel adekvaatse ja ajakohase info sertifikaadiinfo avaldamise kohta.

2.4.3. Juurdepääsureeglid

Juurdepääs punktis 2.4.1 kirjeldatud informatsioonile üldkasutatavat andmesidevõrku kasutades on tasuta ning juurdepääsu ei piirata. Teistel avaldamisviisidel võib SK kehtestada hinnakirjaga määratava tasu ja/või nõuda teeninduslepingu olemasolu.

2.4.4. Kataloogiteenus

SK poolt väljastatud tühistusnimekirjad ja kehtivad sertifikaadid on avaldatud sertifitseerimispoliitikas toodud korra kohaselt avalikus kataloogis aadressil ldap://ldap.sk.ee.

Tühistusnimekirjade koopiad asuvad aadressil http://www.sk.ee/crls.

Kataloogistruktuur ja kasutamiseks vajalikud juhised on toodud SK koduleheküljel.

2.5. Audit

SK tööd auditeeritakse järgnevalt:

- SK tegevus auditeeritakse kord aastas vastavalt teede- ja sideministri 3. oktoobri 2000. a määrusele nr 83, "Teenuse osutajate infosüsteemide auditeerimise kord";
- kord poolaastas viiakse läbi sisemine audit siseaudiitori poolt;
- oluliste teenuste ja infosüsteemi muudatuste korral auditeeritakse infosüsteem välisaudiitori poolt.

Auditeerimise alla kuuluvad järgmised valdkonnad:

a) teenuse kvaliteet;
b) teenuste turvalisus:
c) SK operatsioonide ja protseduuride turvalisus:
d) SK kliendiandmete kaitse ja SK turvapoliitika, tööprotseduuride ja lepinguliste kohustuste ning CPS-i ja sertifitseerimispoliitikate nõuete korrektne täitmine;

Auditi tulemused avaldatakse SK koduleheküljel.

2.6. Konfidentsiaalsus

2.6.1. Konfidentsiaalne informatsioon

Kogu sertifitseerimisteenuse osutamisel teatavaks saanud ning avaldamisele mittekuuluv informatsioon (näiteks SK toimimise tehnilisi üksikasju käsitlev info) on konfidentsiaalne.

Konfidentsiaalse informatsiooni avalikustamine või edastamine kolmandale poolele on lubatud üksnes informatsiooni õigusliku valdaja kirjalikul loal, kohtu otsuse põhjal või teistel õigusaktides sätestatud juhtudel.

2.6.2. Avalik informatsioon

Avaliku informatsiooni alla kuuluvad järgmised materjalid:

- sertifitseerimispõhimõtted koos viidatavate dokumentidega;
- sertifitseerimispoliitikad koos viidatavate dokumentidega;
- kohustusliku kindlustuslepingu tingimused;
- isikuandmete kaitse põhimõtted;
- SK avalikud võtmed ja vastavad teenusesertifikaadid;
- auditeerimistulemused;
- väljastatud sertifikaatide kehtivusinfo.

Avalikule informatsioonile tagatakse juurdepääs punkti 2.4.3 kohaselt.

2.6.3. Isikuandmete kaitse

SK isikuandmete kaitse põhimõtted on toodud dokumendis “Isikuandmekaitse põhimõtted” [4]. Isikuandmete kaitsepõhimõtete täitmise tagamisega garanteeritakse avaldamisele mittekuuluva informatsiooni konfidentsiaalsus, kliendiinformatsiooni kogumise põhjendatus ning isikuandmete kaitse seaduse [5] ja avaliku teabe seaduse [1] täitmine.

3. Kliendi identifitseerimine

3.1. Kliendi isikusamasuse kontroll

Kliendi isikusamasust kontrollitakse vastavalt sertifitseerimispoliitikas määratud isikusamasuse kontrolli protseduuridele.

3.2. Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord

Sertifikaadi taotleja avalikule võtmele vastava isikliku võtme tõendamise kord on toodud sertifikaadiga seotud sertifitseerimispoliitikas.

3.3. Eraldusnimi

Kliendi eraldusnimi koostatakse vastavalt sertifitseerimispoliitikas määratud sertifikaadi- ja tühistusnimekirja profiilile.

SK tagab kliendi eraldusnime ja sertifikaadi kinnitamisel kasutatud SK isikliku võtmega seotud sertifikaadi eraldusnime kombinatsiooni unikaalsuse.

SK kannab väljastatavatesse sertifikaatidesse sertifitseerija kohta unikaalse sertifikaadi järjenumbri.

4. Sertifitseerimisteenuse osutamine. Sertifitseerimismenetluse kord ja tähtajad.

4.1. Sertifikaaditaotluse esitamine

Sertifikaadi taotlemine on võimalik ainult SK klienditeeninduspunktis kui sertifitseerimispoliitikas pole määratletud teisiti.

Täpsema sertifikaadi taotlemise korra määrab ära sertifitseerimispoliitika.

Digitaalallkirja võimaldava sertifikaadi taotluse esitamise kord peab minimaalselt olema kooskõlas DAS-iga ning lisaks järgnevate punktidega:

- Sertifikaaditaotlus peab sisaldama vähemalt järgnevaid punkte:
  - viide taotletava sertifikaadi sertifitseerimispoliitikale;
  - märge selle kohta, kuidas toimub võtmepaari genereerimine;
  - märge selle kohta, et klient volitab SK genereerima kliendi avalikule võtmele vastava sertifikaadi;
  - viide teavituskanalile, mille kaudu edastatakse kliendile sertifitseerimisteenuse osutamisel tekkinud informatsiooni (nt informatsiooni sertifikaadi kehtivuse peatamise kohta);
  - kinnitus selle kohta, et klient aktsepteerib sertifitseerimispõhimõtteid, sertifitseerimispoliitikat ning muid sertifikaatide kasutusala ning sellest tulenevat vastutust kirjeldavaid dokumente.
- Klient täidab sertifikaaditaotluse ja allkirjastab selle;
- Klienditeeninduspunkti töötaja kontrollib avalduse allkirjastanud kliendi isikusamasuse vastavalt punktis 3.1 sätestatule.

4.2. Sertifikaaditaotluse menetlemine

Sertifikaaditaotluse täpne läbivaatamise kord ja töötlemise tähtajad määratakse ära vastavas sertifitseerimispoliitikas. Sertifikaaditaotluse menetlemisel kontrollitakse kliendi poolt esitatud andmete õigsust ja täielikkust.

4.2.1. Otsuse tegemine

Sertifikaaditaotluse rahuldamise või mitterahuldamise otsustab SK või sertifitseerimispoliitikas sätestatud SK lepingujärgne partner maksimaalselt 5 tööpäeva jooksul.

SK või sertifitseerimispoliitikas sätestatud SK lepingujärgne partner lähtub otsuse langetamisel:

- kas kliendil on vastavalt Eesti Vabariigi õigusaktidele õigus saada sertifikaat;
- kas klient on esitanud taotluses enda kohta õigeid ja täielikke andmeid;
- kas klient ei oma sama kasutusvaldkonna ja eraldusnimega sertifikaati.

Klienti teavitatakse otsusest sertifitseerimispoliitikas toodud või sertifikaaditaotluses märgitud teavituskanali kaudu.

4.2.2. Sertifikaadi väljastamine

SK väljastab peale SK klienditeeninduspunkti poolt edastatud sertifikaaditaotluse autentsuse ja terviklikkuse kontrolli taotlusele vastavad sertifikaadid, mis antakse kliendile üle vastavalt sertifitseerimispoliitikas kehtestatud korrale.

4.2.3. Sertifikaatide üle arvestuse pidamise kord

Kõik väljastatud sertifikaadid hoitakse SK suletud infosüsteemi osas olevas sertifikaatide andmebaasis.

Sertifikaadi väljastamisel vastavalt sertifitseerimispoliitikas toodud korrale salvestatakse sertifikaadi koopia avalikus kataloogis, mis on avalikus andmesidevõrgus ööpäevaringselt kättesaadav kõigile teenuse kasutajatele. Kataloogi kaudu on tagatud juurdepääs kõikidele kehtivatele sertifikaatidele ja tühistusnimekirjadele. Kataloogile võib vajadusel juurdepääsu piirata, kui seda nõuavad sertifitseerimispoliitika ja nõuded süsteemi käideldavusele.

4.2.4. Sertifikaadi kehtivuse kontroll ja tõendamine

Huvitatud isiku nõudmisel tõendab SK esindaja enda digitaalallkirjaga SK poolt väljastatud sertifikaadis sisalduvale avalikule võtmele vastava isikliku võtmega antud digitaalallkirja kehtivust.

Sertifikaatide kehtivuskinnituste väljastamisel kasutatavad andmeformaadid, teenuse hinna ja osutamise ajalised piirangud määrab SK. Täpsed tingimused avaldatakse SK koduleheküljel.

4.2.5. Sertifikaadi uuendamine

Sertifikaadi uuendamise tingimused ja sellega seotud protseduurid ning tähtajad tuuakse ära sertifikaadi sertifitseerimispoliitikas.

Sertifikaadi sertifitseerimispoliitika peab tooma välja järgmised uuendamisvõimalused:

a) sertifikaadi uuendamine sertifikaadi aegumise järel;
b) sertifikaadi uuendamine sertifikaadi kehtetuks tunnistamise järel.

Need uuendamisvõimalused peavad sisaldama informatsiooni selle kohta, kas uus sertifikaat antakse välja samale võtmepaarile või mitte.

4.3. Sertifikaadi kehtivuse peatamise ja kehtetuks tunnistamise taotlused

4.3.1. Sertifikaadi kehtivuse peatamise ja kehtetuks tunnistamise taotluste volituste kontroll

Sertifikaatide kehtivuse peatamise ja kehtetuks tunnistamise volitusi kontrollitakse vastavalt järgnevale tabelile 1 kui vastav sertifitseerimispoliitika ei ole määratlenud teisiti.

Taotluse esitamisviis	Kehtivuse peatamistaotlus	Kehtivuse peatatuse lõpetamise taotlus	Kehtetuks tunnistamise taotlus
Telefoni teel, helistades SK abiliinile. Sertifikaatide kehtivuse peatamisel küsitakse kehtivuse peatamise taotleja isikuga seotud andmeid ning võrreldakse neid SK infosüsteemis olevate andmetega.	Kehtivus peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärselt vastamise korral.	Ei aktsepteerita. Pakutakse kliendile sobiv kanal kehtivuse peatatuse lõpetamise taotluse esitamiseks.	Kehtivus peatatakse isikuandmeid puudutavatele kontrollküsimustele usaldusväärselt vastamise korral ning pakutakse kliendile sobiv kanal kehtetuks tunnistamise taotluse esitamiseks.
SK klienditeeninduspunktis isikut tõendava dokumendi esitamisel.	Kehtivus peatatakse.	Kehtivuse peatatus lõpetatakse	Tunnistatakse kehtetuks.

Tabel 1. Kehtivuse peatamise ja kehtetuks tunnistamise volitused

4.3.2. Kehtetuks tunnistatud, peatatud kehtivusega või aegunud sertifikaadi õigusliku kasutamise välistamine

Kehtetuks tunnistatud, peatatud kehtivusega või aegunud sertifikaadi õigusliku kasutamise välistamine tagatakse peale sertifikaadi kehtetuks tunnistamist või aegumist selle kataloogist kustutamisega ja arhiveerimisega SK infosüsteemis.

Kehtetuks tunnistatud või peatatud kehtivusega sertifikaat publitseeritakse tühistusnimekirjas peale selle sertifikaadi kehtetuks tunnistamist või kehtivuse peatamist.

4.3.3. Sertifikaadi õigusliku aluseta kehtetuks tunnistamise tagajärjed

Isik või asutus, kelle tahtluse või raske ettevaatamatuse tõttu on sertifikaat tunnistatud ilma õigusliku aluseta kehtetuks, on kohustatud hüvitama sertifikaadi kehtetuks tunnistamisega tekkinud otsese kahju.

4.4. Sertifikaatide kehtivuse peatamine

4.4.1. Sertifikaadi kehtivuse peatamise tingimused ja menetlus

4.4.1.1. Tingimused sertifikaadi kehtivuse peatamiseks

Täpsed tingimused sertifikaadi kehtivuse peatamise kohta tuuakse sertifikaadile vastavas sertifitseerimispoliitikas. Sertifikaadi kehtivuse peatamisvõimalus peab olema toodud ära digitaalallkirja võimaldavates sertifitseerimispoliitikates.

Vastavalt DAS-ile [2] sertifikaadi kehtivus peatatakse, kui:

- SK-l või sertifitseerimispoliitikas sätestatud SK lepingujärgsel partneril tekib põhjendatud kahtlus, et sertifikaati on kantud ebaõiged andmed või et sertifikaadis sisalduvale avalikule võtmele vastavat isiklikku võtit on võimalik kasutada sertifikaadi omaniku nõusolekuta;
- sertifikaadi kehtivuse peatamist nõuab sertifikaadi omanik või tema notariaalselt kinnitatud volitustega esindaja;
- sertifikaadi kehtivuse peatamist nõuab andmekaitse järelevalveasutus või SRR vastutav töötleja, kui tal tekib põhjendatud kahtlus, et sertifikaati on kantud ebaõiged andmed või et sertifikaadis sisalduvale avalikule võtmele vastavat isiklikku võtit on võimalik kasutada sertifikaadi omaniku nõusolekuta;
- sertifikaadi kehtivuse peatamist nõuab kohus, prokuratuur või kriminaalasjas kohtueelset uurimist teostav asutus kuritegude tõkestamiseks.

4.4.1.2. Sertifikaadi kehtivuse peatamise volitused

Sertifikaadi kehtivust võivad peatada:

- klient (sertifikaadi omanik);
- SK või sertifitseerimispoliitikas sätestatud SK lepingujärgse partneri vastutav töötaja;
- SRR vastutav töötleja;
- DAS-is nimetatud vastava volitustega ametnik kohtueelse uurimise teostamiseks ja kuritegude tõkestamiseks.

4.4.1.3. Kehtivuse peatamistaotluse esitamine

Kehtivuse peatamistaotluse esitaja esitab kirjaliku avalduse sertifikaadi kehtivuse peatamiseks lähimas SK klienditeeninduspunktis.

Kehtivuse peatamistaotlusi saab esitada ka ööpäevaringselt telefoni teel abiliini kaudu.

Informatsiooni klienditeeninduspunktide ja nende lahtiolekuaegade kohta edastatakse SK koduleheküljel.

4.4.1.4. Kehtivuse peatamistaotluse menetlus

Sertifikaadi kehtivuse peatamise volituste kontroll toimub vastavalt esitusviisile tabelis 1 toodud korras. Kui klient esitab taotluse sertifikaadi kehtivuse peatamiseks SK klienditeeninduspunktis, peab ta eelnevalt täitma vastava avaldusblanketi ja allkirjastama selle. Seejärel toimub menetlus alljärgnevalt:

- kontrollitakse kehtivuse peatamistaotleja volitusi;
- kontrollitakse sertifikaadi kehtivuse peatamise avalduse seaduslikkust;
- registreeritakse kehtivuse peatamise kõne abiliini operaatori poolt või registreeritakse kehtivuse peatamine SK klienditeeninduspunkti töötaja poolt;
- kontrollitakse kehtivuse peatamistaotleja isikuga seotud andmeid;
- viiakse läbi sertifikaadi kehtivuse peatamisavalduse käesolevale sertifitseerimispoliitikale vastavuse kontroll SK infosüsteemi poolt;
- sertifikaadi kehtivuse peatamistaotlus registreeritakse SK infosüsteemis;
- sertifikaadi kehtivus märgitakse peatatuks sertifikaatide andmebaasis (tühistusnimekirjas on vastavaks põhjuskoodiks 6 (*hold*));
- sertifikaat kustutatakse avalikust kataloogist;
- antakse välja uus sertifikaatide tühistusnimekiri vastavalt punktis 2.4.2 sätestatule;
- arhiveeritakse kehtivuse peatamistaotluse aluseks olevad materjalid.

Kui kehtivuse peatamine esitati abiliini kaudu, teavitatakse sertifikaadi omanikku sertifikaadi kehtivuse peatamisest kohe peale kehtivuse peatamistoimingu sooritamist. Kliendil on võimalus veenduda kataloogi või tühistusnimekirja põhjal, et sertifikaadi kehtivus on peatatud.

4.4.1.5. Kehtivuse peatamise operatiivsus

Sertifikaadi kehtivuse peatamine kajastub koheselt SK sertifikaatide andmebaasis ja avalikus kataloogis. Kehtivuse peatamise järel väljastab SK vastavalt punktis 2.4.2 toodud korrale uue tühistusnimekirja, mis sisaldab peatatud kehtivusega sertifikaadi järjekorranumbrit.

4.5. Sertifikaadi kehtivuse peatatuse lõpetamine

4.5.1. Tingimused sertifikaadi kehtivuse peatatuse lõpetamiseks

Sertifikaadi kehtivuse peatatus lõpetatakse sertifikaadi omaniku või sertifikaadi kehtivuse peatamist nõudnud isiku või asutuse kirjaliku avalduse alusel vastavate andmete kandmisega sertifikaatide andmebaasi.

Sertifikaadi kehtivuse peatatuse avaldusega kinnitab sertifikaadi omanik, et sertifikaadi kehtivuse peatatuse ajal antud digitaalallkirjad on kehtetud.

4.5.2. Sertifikaadi kehtivuse peatatuse lõpetamise volitused

Sertifikaadi kehtivuse peatatust võivad lõpetada:

- Sertifikaadi kehtivuse peatanud sertifikaadiomanik;
- SRR vastutav töötaja;
- SK või sertifitseerimispoliitikas sätestatud SK lepingujärgse partneri vastutav töötaja;
- vastavalt DAS-ile muu vastava volitustega ametnik, kes tegutses sertifikaadi kehtivuse peatamisel vastavalt punktile 4.4.1.2.

4.5.3. Sertifikaadi kehtivuse peatatuse lõpetamise taotluse esitamine

Sertifikaadi kehtivuse peatatuse lõpetamise taotlus esitatakse kirjalikult täidetud avaldusblanketil peale isikusamasuse kontrolli ja volituste kontrolli SK klienditeeninduspunktis.

Sertifikaadi kehtivuse peatatuse lõpetamise tunnistamise taotlemiseks esitatud avaldus peab sisaldama:

- avalduse esitaja nime;
- avalduse esitaja allkirja;
- peatatud kehtivusega sertifikaadi omaniku nime ja isikukoodi;
- peatatud kehtivusega sertifikaadi väljastanud SK eraldusnime;
- kehtivuse peatatuse lõpetamise alust.

Kui avaldust ei esitanud sertifikaadi omanik, vaid vastavaid volitusi omav ametnik või SK vastutav töötaja, siis peab avaldusele olema lisatud kehtivuse peatatuse lõpetamist lubavad dokumendid.

Avalduse registreerimisel märgitakse üles avalduse esitaja isikusamasuse kontrollil kasutatud dokumendi andmed.

4.5.4. Sertifikaadi kehtivuse peatatuse lõpetamise menetlus

Kehtivuse peatatuse lõpetamise menetlus toimub järgnevalt:

- Kehtivuse peatatuse lõpetamise algataja koostab kirjaliku avalduse sertifikaadi kehtivuse peatatuse lõpetamiseks SK klienditeeninduspunktis vastavale blanketile ja allkirjastab selle;
- kontrollitakse kehtivuse peatatuse lõpetamise volitust;
- kontrollitakse sertifikaadi kehtivuse peatatuse lõpetamise avalduse seaduslikkust;
- viiakse läbi kehtivuse peatatuse lõpetamise vastavuse kontroll SK infosüsteemi poolt;
- registreeritakse sertifikaadi kehtivuse peatatuse lõpetamise fakt SK infosüsteemis;
- avaldatakse sertifikaat uuesti avalikus kataloogis;
- antakse välja uus sertifikaatide tühistusnimekiri vastavalt punktis 2.4.2 sätestatule.

Sertifikaadi omanikku teavitatakse sertifikaadi kehtivuse peatatuse lõpetamise toimingu edukast läbiviimisest koheselt. Kliendil on võimalus veenduda kataloogi või tühistusnimekirja põhjal, et sertifikaat on aktiivne.

4.5.5. Sertifikaadi kehtivuse peatatuse lõpetamise operatiivsus

Sertifikaadi kehtivuse peatamine kajastub koheselt SK sertifikaatide andmebaasis ja avalikus kataloogis. Kehtivuse peatatuse lõpetamise järel väljastab SK vastavalt punktis 2.4.2 toodud korrale uue tühistusnimekirja, mis ei sisalda kehtivuse peatatuse lõpetanud sertifikaadi järjekorranumbrit.

4.6. Sertifikaadi kehtetuks tunnistamine

4.6.1. Sertifikaadi kehtetuks tunnistamise volitused

Sertifikaadi kehtetuks tunnistamise avalduse võib esitada sertifikaadi omanik, tema notariaalselt kinnitatud volitusega esindaja või muu õigusaktides toodud isik.

4.6.2. Sertifikaadi kehtetuks tunnistamise avalduse esitamine

Sertifikaadi kehtetuks tunnistamine toimub kirjaliku avalduse alusel.

Sertifikaadi kehtetuks tunnistamise avaldus peab sisaldama:

- avalduse esitaja nime;
- avalduse esitaja allkirja;
- kehtetuks tunnistatava sertifikaadi omaniku nime ja isikukoodi;
- kehtetuks tunnistatava sertifikaadi väljastanud SK eraldusnime;
- sertifikaadi kehtetuks tunnistamise põhjust;
- vajadusel tõendusmaterjali sertifikaadi kehtetuks tunnistamise põhjuse asjaolude tõendamiseks.

Kehtetuks tunnistamise avalduse esitaja identifitseeritakse SK klienditeeninduspunktis kehtiva isikut tõendava dokumendi alusel. Avalduse registreerimisel märgitakse üles avalduse esitaja identifitseerimisel kasutatud dokumendi andmed.

4.6.3. Sertifikaadi kehtetuks tunnistamise menetlus

Sertifikaadi kehtetuks tunnistamise menetlus toimub järgnevalt:

- sertifikaadi kehtetuks tunnistamise taotleja koostab kirjalikult sertifikaadi kehtetuks tunnistamise avalduse SK klienditeeninduspunktis vastavale blanketile ja allkirjastab selle;
- kontrollitakse sertifikaadi kehtetuks tunnistamise avalduse seaduslikkust;
- viiakse läbi kehtetuks tunnistamise avalduse õigsuse kontroll SK infosüsteemi poolt;
- sertifikaadi kehtetuks tunnistamise avaldus registreeritakse SK infosüsteemis;
- sertifikaat märgitakse kehtetuks avalikus kataloogis;
- antakse välja uus sertifikaatide tühistusnimekiri vastavalt punktis 2.4.2 sätestatule;
- arhiveeritakse kehtetuks tunnistamise avalduse aluseks olevad materjalid.

Kliendil on võimalus veenduda avaliku kataloogi või tühistusnimekirja põhjal, et sertifikaat on tunnistatud kehtetuks.

4.6.4. Sertifikaadi kehtetuks tunnistamise menetluse operatiivsus

Sertifikaadi kehtetuks tunnistamine kajastub koheselt SK sertifikaatide andmebaasis ning avalikus kataloogis. Peale sertifikaadi kehtetuks tunnistamist väljastab SK vastavalt punktis 2.4.2 toodud korrale uue tühistusnimekirja, mis sisaldab kehtetuks tunnistatud sertifikaadi järjekorranumbrit.

4.7. Protseduurid jälgitavuse tagamiseks

4.7.1. Dokumentide säilitamine

Sertifitseerimisteenuse osutamisega seotud dokumentatsiooni säilitab SK kuni oma tegevuse lõpuni.

Sertifikaatide kehtetuks tunnistamise põhjust tõestavad dokumendid säilitatakse kuni SK tegevuse lõpuni, kui seaduses ei ole sätestatud teisiti.

Kui SK-le on esitatud sertifikaadi kohta pretensioon või kui sertifikaat on tõendusmaterjaliks kohtulikus vaidluses, siis selle sertifikaadi kohta käivat informatsiooni ja dokumentatsiooni säilitatakse lõpliku lahenduseni jõudmiseni.

SK teenuste osutamise lõpetamise järel antakse vastavalt seadusandlusele ja kehtestatud korrale kogu digitaalallkirja võimaldavate sertifikaatidega seotud dokumentatsioon üle SRR-ile.

4.7.2. Logi

SK infosüsteemid logivad:

- kõiki SK kinnitusvõtmete elutsükli etappe ja kasutamist;
- kõiki klientide võtmete elutsükli etappe;
- kõiki turvasündmusi, nagu näiteks kasutajate autoriseerimised või edutud autoriseerimise katsed;
- eriõigustega süsteemikasutajate tegevusi.

SK kasutab standarditele vastavaid infoturbelahendusi, mis tagavad isiklike võtmete, aktiveerimiskoodide, pääsukoodide (näiteks PIN-ide) ja muu turvakriitilise informatsiooni logis mittesalvestumise.

Kõik intsidendid, eriolukorrad ja probleemid registreeritakse ning olulisusest ja iseloomust sõltuvalt edastatakse edasisele käsitlemisele vastavalt SK sisemistele kordadele.

Logid säilitatakse SK infosüsteemis vähemalt 36 kuud.

SK tagab infotehnoloogiliste ja organisatsiooniliste vahenditega logi muutmatuse, säilimise ja konfidentsiaalsuse.

SK-s on kehtestatud kord logide regulaarseks analüüsiks ning võimaliku ründe kiireks avastamiseks.

4.7.3. Turvaline logi

SK infosüsteemis on rakendatud spetsiaalne turvalise logi süsteem, mis tagab krüptograafiliste meetoditega logikirjete ajalise järjestuse tervikluse. Turvalisse logisse kantakse:

- kõik sertifikaatide olekumuutused (aktiveerimine, kehtivuse peatamine, kehtivuse peatatuse lõpetamine, kehtetuks tunnistamine)
- kõik SK poolt välja antavad sertifikaatide kehtivuskinnitused

Salgamise vääramise tagamiseks publitseeritakse turvalise logi ühte kirjet vähemalt üks kord aastas SK kodulehel ning vähemalt ühes üleriigilises päevalehes.

Turvaline logi tagab sertifikaatide olekuinformatsiooni auditeeritavuse. SK kodulehel paikneva rakenduse abil on Kliendil võimalik turvaliselt näha tema sertifikaatidega sooritatud olekumuutusi ja nende kohta väljastatud kehtivuskinnitusi.

4.8. Tegutsemine eriolukorras

SK on koostanud riskianalüüsi SK sertifitseerimissüsteemi kohta, et ennetada võimalikku ohtu SK tegevuse käideldavusele.

SK kasutab teenuse osutamisel tehnilisi vahendeid ja infosüsteemi turbemeetodeid, et minimiseerida sertifitseerimisteenuse oma kontrolli alt väljumise ohtu.

SK kehtestab sisemised korrad, juhendid ja taasteplaanid kriisisituatsioonis tegutsemiseks, tagamaks teenuse osutamise turvalisus ja kvaliteet.

AS-i Sertifitseerimiskeskus infosüsteem ja kasutatav dokumentatsioon on auditeeritud sõltumatu IT audiitori poolt.

Sertifitseerimisteenuse osutamisel loetakse olulisimateks eriolukordadeks alljärgnevaid juhtumeid:

- SK sertifitseerimiseks kasutatava isikliku võtme väljumine SK kontrolli alt või tekkinud on tõsine kahtlus kontrolli alt väljumise kohta;
- SK sertifikaatide andmebaasi hävimine;
- andmetöötluskeskust (serveriruum) sisaldava hoone täielik või osaline hävimine;
- andmetöötluskeskust (serveriruum) avaliku andmesidevõrgu ühendava sidekanali tõrge, mille tulemusel pole võimalik teenust osutada;
- veevärgi, jahutusseadmete või UPS-i tõrge andmetöötluskeskuses (serveriruum);
- tulekahju SK bürooruumides ja/või andmetöötluskeskuses (serveriruum);
- teenuse tõkestamiseks teostatud infotehnoloogiline rünne;
- olulise personaliosa üheaegne töövõimetus.

Nimetatud eriolukordade kohta koostatakse taasteplaanid.

Ülaltoodud eriolukordade lahendamine ja teenuse taastamine toimub kehtiva SK eriolukordade lahendamise korra ja nimetatud eriolukordade kohta koostatud taasteplaanide alusel.

Muud teenuse osutamise käigus tekkinud eriolukorrad lahendatakse vastavalt SK kehtivale eriolukordade lahendamise korrale.

Tegutsemiskavades esitatakse teenuse osutamiseks vajalike minimaalsed kvaliteedinõuded tegutsemiseks *force majeure'i* tingimustes.

Eriolukorra ilmnemise korral teavitab SK viivitamatult, vähemalt ilmnemisele järgneva tööpäeva jooksul, teenuse kasutajaid tekkinud eriolukorrast ja planeeritud lahenduskavast avalike teabelevituskanalite kaudu.

Kui eriolukorra tõttu sai võimalikuks sertifikaadi andmebaasi sisu muutumine, sertifikaatide väljastamine, kehtivuse peatamine, kehtivuse peatatuse lõpetamine, kehtetuks tunnistamine, siis SK taastab viivitamatult, vähemalt ilmnemisele järgneva ööpäeva jooksul, eriolukorrale eelnenud sertifikaatide andmebaasi seisu ja teavitab sellest sertifikaadi omanikke oma koduleheküljel.

4.9. Sertifitseerimisteenuse osutaja töö lõpetamine

Sertifitseerimisteenuse osutamine lõpetatakse:

a) SK nõukogu otsusega;
b) teenuse osutamise üle järelevalvet teostava asutuse otsusega;
c) kohtuotsusega;
d) AS-i Sertifitseerimiskeskus likvideerimise või tegevuse lõpetamise korral.

Sertifitseerimisteenuse osutamise lõpetamisel annab SK teenuse osutamisega seotud dokumentatsiooni üle SRR-ile vastavalt kehtestatud korrale.

SK teenuse lõpetamisest teavitatakse SK koduleheküljel http://www.sk.ee .

SK kohustub lisaks DAS-is esitatud nõuetele teenuse lõpetamisel tunnistama kehtetuks kõik väljaantud ja kehtivad sertifikaadid.

SK valduses olevad riistvaralised seadmed kas reinitsialiseeritakse või hävitatakse, sõltuvalt konkreetsest turvalisuse nõuetest.

SK ei vastuta teenuse lõpetamisel teenuse kasutajale tekkida võivate mistahes kahjude eest, kui SK on sellest avaliku teabekanali kaudu teatanud vähemalt 1 kuu enne teenuse osutamise lõpetamist.

5. Füüsilised ja organisatsioonilised turbemeetmed

5.1. Turbehaldus

SK juhindub turbe haldamisel tunnustatud standarditest, nt ISO 13335, ISO 13569.

SK juhtkond kehtestab turvapoliitika, mis on infoturbe järjepidevuse, täielikkuse ja juhtkonna toetuse aluseks.

SK haldab infovarade registrit ning klassifitseerib kõik infovarad turbeklassidesse vastavalt turvaanalüüsi tulemustele. Kõigil olulistel infovaradel on määratud vastutaja.

SK infoturbe dokumentatsiooni täitmist jälgitakse korraliste auditite käigus sõltumatu audiitori poolt.

5.2. Füüsilised turbemeetmed

5.2.1. SK füüsiline pääsukontroll

Pääs SK ruumidesse on piiratud.

SK ruumides kasutatakse füüsilist või elektroonilist valvet.

SK andmetöötluskeskustesse tohivad SK töötajad siseneda üksnes kinnitatud nimekirja alusel. Kõigi SK andmetöötluskeskusesse sisenemiste kohta peetakse päevikut.

Teisaldatava meedia, seadmete ja tarkvara SK ruumidest väljaviimine toimub kehtestatud korra alusel. Andmekandjaid tundliku informatsiooniga tohib säilitada üksnes spetsiaalses andmekandjate hoidmiseks määratud tulekindlas seifis.

5.3. Nõuded tööprotseduuridele

SK infosüsteemi kasutatakse üksnes sihipäraselt.

Arenduseks ja testimiseks kasutatakse töösüsteemist eraldatud ning sõltumatut infosüsteemi koos täielikult sõltumatute isiklike võtmete, paroolide, koodide ja teiste pääsutunnustega.

5.3.1. Oluliste toimingute läbiviimine

5.3.1.1. Jagatud kontroll

Sertifikaatide kinnitamiseks kasutatava SK sertifikaadi ning isikliku võtme aktiveerimine toimub jagatud kontrolli alusel. Vastavad kontrolli meetmed kehtestatakse SK sisemiste protseduurireeglitega.

5.3.1.2. Toimingute dokumenteerimine

Turvalisuse aspektist oluliste toimingute sooritamise kohta koostatakse akt. Need toimingud peavad vähemalt sisaldama:

- kõiki SK tipmise sertifitseerija kinnitamisvõtme elutsükli etappe ja kasutuskordasid;
- kõiki SK alamate sertifitseerijate kinnitamisvõtme elutsükli etappe;
- eriolukordade lahendusi.

5.4. Personali turbenõuded

Töötajal, kes on seotud käesolevas CPS-is kirjeldatud teenuse osutamisega, ei tohi olla karistatust tahtlikult toime pandud kuriteo eest. Töötajad peavad olema piisavalt koolitatud ning omama vajalikke kogemusi töölepingus ja ametijuhendis ettenähtud töö tegemiseks.

SK töötajate töölepingutes on kohustus hoida saladuses töö käigus teatavaks saanud konfidentsiaalset informatsiooni vähemalt viis aastat peale töölepingu lõppemist.

SK töötajad ei tohi omada ärihuve konkureerivas ettevõttes, mis võivad mõjutada nende otsuseid teenuse osutamisel.

SK töötajatel peavad olema ametijuhendid, milles on ära märgitud järgnevatesse turvakriitilistesse rollidesse kuulumine:

- infoturbeülem: vastutav infoturbepoliitika koostamise ja elluviimise eest;
- süsteemiadministraator: vastutav SK infosüsteemi paigaldamise, konfigureerimise ja haldamise eest; ei oma juurdepääsu turvakriitilisele informatsioonile;
- süsteemioperaator: vastutav SK infosüsteemi igapäevase halduse eest, sh varukoopiate tegemine ning süsteemi taastamine.
- siseaudiitor: omab õigust jälgida dokumendiarhiive ja infosüsteemide logisid.

Turvakriitiliseks informatsiooniks nimetatakse informatsiooni, mis võimaldab teenuse taasloomist, jäljendamist, kinnitusvõtme avalikustamist või hävitamist.

Vähemalt infoturbeülema, siseaudiitori ja süsteemiadministraatori rollid peavad olema täielikult eraldatud ning täidetud erinevate isikute poolt.

6. Tehnilised turbenõuded

6.1. Võtmehaldus

6.1.1. SK kinnitusvõtmed

6.1.1.1. SK kinnitusvõtmete loomine

Sertifitseerimisteenuse osutamisel kasutatakse RSA algoritmi võtmeid järgmiste miinimumpikkustega:

- SK kinnitusvõti – 2048 bitti;
- sertifikaadile vastav isiklik võti – 1024 bitti.

Sertifitseerimisteenuse osutamiseks vajalikud SK kinnitusvõtmed luuakse vastavalt SK sisekorra dokumentidele „SK juurvõtme loomise protseduur" ja „SK alamsertifitseerijate võtmete loomise protseduur". SK võtmete loomist jälgib komisjon, kes koostab peale võtmete loomist vastavasisulise akti, mis sisaldab võtmepaarile loodud sertifikaadi avaliku võtit ja räsi. Võtmete loomise akt avaldatakse keskuse koduleheküljel.

6.1.1.2. Võtmete kaitse

Käideldavusnõuete rahuldamiseks luuakse SK kinnitusvõtmetest varukoopia. Võti jagatakse kolmeks osaks, mida säilitavad erinevad isikud. SK kinnitusvõtme säilitamisel kasutatakse turvaümbrikku, mille avamine on tuvastatav.

SK kinnitusvõtmed on kasutatavad üksnes aktiveeritud olekus. SK kinnitusvõtme aktiveerimiseks on vajalik vähemalt kahe volitatud isiku osavõtt.

SK kinnitusvõtmed deaktiveeruvad võtmete säilitamisel kasutatava turvamooduli avamise katsel, konfiguratsiooni muutmisel, vooluvõrgust eemaldamisel, teisaldamisel ja teistel turvalisust ohustada võivatel sündmustel.

Sertifitseerimisteenuse osutamisel kasutatavad turvamoodulid vastavad minimaalselt turvastandardis *FIPS PUB 140-1 Level 3* toodud nõuetele.

6.1.1.3. SK kinnitusvõtme hävitamine

SK kinnitusvõtmetest hävitatakse aegumise või kehtetuks tunnistamise järel kõik koopiad nii, et nende edasine kasutamine või tuletamine on võimatu.

6.1.2. Kliendi võtmed

6.1.2.1. Kliendi võtmete moodustamine

Kliendi võtmete moodustamine toimub vastavalt sertifikaadi sertifitseerimispoliitikas toodud põhimõtete järgi.

Kliendi võtmed peavad olema kaitstud ainult kliendile teadaolevate PIN koodidega e aktiveerimiskoodidega.

6.1.2.2. Kliendi isikliku võtme ja aktiveerimiskoodide kaitse valmendamise käigus

Kui kliendi isiklikud võtmed genereerib SK, siis peab olema tagatud genereeritud kliendi isikliku võtme ning aktiveerimiskoodide konfidentsiaalsus ja volitusteta mittekasutamine kuni nende kliendile üleandmiseni.

Aktiveerimiskoodid trükitakse ühes eksemplaris. Aktiveerimiskoodid kaitstakse selliselt, et neid ei ole võimalik lugeda ilma turvaelementi rikkumata. Kliendil on kohustus keelduda rikutud turvaelemendiga aktiveerimiskoodide vastuvõtmisest.

SK-l ei ole käesoleva CPS-i mõttes mingit vastutust kliendi võtme ja selle aktiveerimiskoodi konfidentsiaalsuse eest juhul, kui kliendi võtmed genereerib klient ise või teeb seda selle vastutuse võtnud kolmas osapool.

6.1.2.3. Kliendi isikliku võtme aktiveerimine

Igakordne isikliku võtme aktiveerimine eeldab aktiveerimiskoodi sisestamist. Kliendi erinevatele võtmetele peab olema võimalik kehtestada erinevaid aktiveerimiskoode.

Aktiveerimiskoodid peavad vastama järgmistele tingimustele:

- aktiveerimiskoodid on kliendile muudetavad;
- aktiveerimiskoodide pikkus ei tohi olla lühem kui 4 sümbolit;
- aktiveerimiskoode käsitlevate tarkvara- ja riistvarakomponentide terviklus peab olema tagatud;
- aktiveerimiskoodi sisestamisel peab olema võimalik seda teha kolmandate isikute eest varjatult;
- isikliku võtme aktiveerimise ajal peab klient olema teadlik sooritatavast tegevusest: digitaalallkirja andmisel tuleb esitada allkirjastatava dokumendi sisu.

SK-l ei ole käesoleva CPS-i mõttes mingit vastutust kliendi isikliku võtme aktiveerimise turvalisuse eest.

6.1.2.4. Kliendi võtmete hävitamine

Kliendi võtmete hävitamine on määratud vastava sertifitseerimispoliitikaga. Juhul, kui SK on kliendi võtmeid varundanud, hävitab SK sertifikaadi kehtivuse lõppemise või kehtetuks tunnistamise järel vastava kliendi võtme.

6.1.2.5. Kliendi võtmete varundamine ja deponeerimine

Klientide isiklikest võtmetest ei salvestata varukoopiaid ja neid ei deponeerita mingil moel juhul, kui vastavat isiklikku võtit kasutatakse digitaalallkirja andmiseks. Muudel juhtudel võidakse kliendi võtmeid deponeerida ja teha neist varukoopiad juhul, kui klient esitab sellise soovi ning selline teenus on ette nähtud sertifitseerimispoliitikaga.

6.2. Süsteemiturve

6.2.1. Pääsukontroll

SK kasutab pääsukontrollisüsteemi, mis identifitseerib, autoriseerib ja registreerib usaldusväärselt kõik SK infosüsteemi kasutajad, ka SK klienditeeninduspunkti töötajad.

6.2.2. Tarkvara turve

SK infosüsteemis, sh kõigis töökohtades on rakendatud meetmeid tarkvara ja konfiguratsiooni terviklikkuse tagamiseks ja pahatahtliku tarkvara tuvastamiseks ning levimise piiramiseks.

Infosüsteemis kasutatakse üksnes otseselt tööülesannete täitmiseks vajalikku tarkvara, mis on kooskõlastatud infoturbejuhiga ja pärineb usaldusväärsest allikast.

6.2.3. Võrguühenduste turve

Tundlike andmete edastamine üle SK välise võrgu on krüpteeritud.

SK sisevõrgu kaabeldus ja aktiivseadmed koos konfiguratsiooniga on kaitstud füüsiliste ja organisatsiooniliste meetmetega.

SK sisevõrgu ning välisühenduste turvalisust jälgitakse pidevalt.

6.2.4. Kellaaegade sünkroniseerimine

Sertifitseerimisteenuse osutamise süsteemi kõigi osade kellaaegade maksimaalne erinevus on kuni üks sekund.

Selle tagamiseks on kasutusel sisemine etalonkella teenus, mille järgi sünkroniseeritakse kõikide sertifitseerimisteenuse osutamise süsteemi osade ajaarvamist.

Etalonkella sünkroniseeritakse GPS (*Global Positioning System*) abil, mis määrab ära ka etalonkella täpsuse.

6.3. Sertifitseerimisteenuse osutamiseks kasutatavate tehniliste vahendite kirjeldus

SK kasutab sertifitseerimisteenuse osutamisel firma Baltimore Technologies ITSEC-3 sertifitseeritud sertifitseerimistarkvara *Unicert*. Sertifikaatide väljastamine (genereerimine) toimub kaitstud võrgusegmendis nn tootekeskkonnas paiknevas ainult selleks otstarbeks eraldatud sertifitseerimisserveri sertifitseerijamoodulis CA.

Sertifitseerimismooduli CA juhtimine toimub operaatormooduli CAO kaudu, mida saavad kasutada ainult selleks volitatud operaatorid sertifitseerimisserveri juures asuva konsooli abil. Sertifitseerimismooduli isiklike võtmete turvaliseks säilitamiseks on kasutusel turvamoodul, mis vastab *FIPS Pub 140-1 Level 3* standardile.

Sertifikaaditaotluste töötlus toimub selleks eraldatud registreerimismoodulis RA, mille juhtimise tarkvarana kasutatakse laiendatud võimalustega registreerimisoperaatorit ARM.

6.4. Sertifitseerimisteenuse osutamisel tekkinud andmete säilitamine ja kaitse

SK hoiab ja arhiveerib elektrooniliselt informatsiooni kõigi sertifikaatide ja nende staatuse muudatustega seotud toimingute kohta. Andmete varukoopiaid hoitakse turvaliselt kahes erinevas asukohas.

Andmekaitsepõhimõtted on toodud dokumendis “Isikuandmete kaitse põhimõtted”.
SK säilitab sertifitseerimisteenuse osutamisel tekkinud andmeid oma tegevusaja lõpuni.

7. Sertifikaatide ja tühistusnimekirjadele (CRL-ide) tehnilised profiilid

7.1. Sertifikaatide profiil

Sertifikaadiprofiilid on avaldatud või viidatud vastavates sertifitseerimispoliitika dokumentides.

Sertifitseerijate sertifikaatide profiilid on esitatud dokumendis “AS-i Sertifitseerimiskeskus CA sertifikaatide profiilid”.

Sertifikaadi profiil peab olema koostatud vastavalt RFC 3280-s [6] esitatud nõuetele.

7.2. Tühistusnimekirjad (CRL)

SK väljastab tühistusnimekirju vastavalt RFC 3280-s [6] esitatud nõuetele. Sertifitseerimispoliitika võib tühistusnimekirjade nõudeid vajadusel täpsustada.

8. Sertifitseerimispõhimõtete haldus

Sertifitseerimispõhimõtete sisulist tähendust mitte muutvate paranduste puhul, nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, tuleb muudatused dokumenteerida käesoleva dokumendi „Versiooni info“-sektsioonis ning suurendada dokumendi versiooninumbri murdarvulist osa.

Sisuliste muudatuste puhul peab uus sertifitseerimispõhimõtete versioon olema eelnevatest selgelt eristatav. Uus versioon peab kandma ühe võrra suurendatud versiooninumbrit. Muudetud sertifitseerimispõhimõtted koos kehtima hakkamise päevaga, mis ei või olla varasem kui 30 päeva avaldamisest, tuleb avaldada elektrooniliselt SK koduleheküljel.

Kõik muudatused kooskõlastatakse SR-ga.

9. Viidatud dokumendid

[1] Avaliku teabe seadus, RT I 2000, 92, 597
[2] Digitaalallkirja seadus, RT I 2000, 26, 150
[3] Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365
[4] Isikuandmete kaitse põhimõtted, AS Sertifitseerimiskeskus
[5] Isikuandmete kaitse seadus RT I 2007, 24, 127
[6] RFC 3280 – Request For Comments 3280, Internet X.509 Public Key Infrastructure / Certificate and Certificate Revocation List (CRL) Profile
[7] RFC 2527 – Request For Comments 2527, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

10. Kasutatud termonoloogia

Käesolevas CPS-is kasutatakse termineid alljärgnevas mõistes. Mõistete definitsioonid ei pruugi kokku langeda DAS-is defineeritud mõistetega.

Termin	Definitsioon
Autentimine	Isiku ühene identifitseerimine tema väidetavat identiteeti kontrollides
Avalik võti	Digitaalallkirja kontrollimise vahend
Digitaalallkiri	Andmekogumile lisatud andmed või rakendatud transformatsioon, mis võimaldab andmekogumi saajal teha kindlaks andmete allikat ja terviklust ning kaitsta võltsimise eest
Eraldusnimi	Unikaalne, üheselt objekti identifitseeriv identifikaator
Eriõigustega süsteemikasutaja	Süsteemiadministraator; arvutisüsteemi kasutaja, kes ei allu tavapärastele õiguste piirangutele süsteemi haldamise võimaldamiseks
Huvitatud isik	(*Relying Party*) Osapool, kes võtab digitaalallkirja põhjal vastu mingi otsuse, vt punkt 2.1.4
Isik	DAS-i mõistes füüsiline isik. DAS-i väliselt võib käesoleva CPS-i mõistes käsitleda isikuna ka juriidilist isikut juhul, kui ei väljastata sertifikaate digitaalseks allkirjastamiseks
Isiklik võti	Isiku valduses olev võti, mille abil tõendab ta oma isikut (digitaalallkirja andmise vahend)
Kataloogiteenus	Sertifikaatide kehtivusinfo edastamise teenus
Kinnitusvõti	Sertifitseerimisteenuse osutaja isiklik võti, mida kasutatakse sertifikaatide signeerimiseks
Klienditeeninduspunkt	Käesolevale CPS-ile vastava sertifitseerimispoliitika alusel toimiv SK teeninduspunkt sertifitseerimisega seotud teenuste osutamiseks, vt punkt 1.2.2.1
Klient	Sertifikaadi omanik, vt punkt 1.2.3.1
Krüpteerimine	Informatsiooni töötlusviis, mille puhul muudetakse informatsiooni loetamatuks neile, kes ei oma selleks vajalikke teadmisi või õigusi
Objektiidentifikaator	(OID) Ühene identifitseerimisnumber mingi objekti, näiteks sertifitseerimispoliitika ja sertifitseerimispõhimõtete identifitseerimiseks
Räsifunktsioon	Matemaatiline teisendus, mille alusel viiakse sõnum (suvaline andmekogum) vastavaks fikseeritud pikkusega andmekogumiga – sõnumilühendiga. Raske on leida kahte erinevat sõnumit, mille sõnumilühendid ühtivad
Sertifikaaditaotlus	Kliendi poolt täidetav ning käsitsi allkirjastatav kirjalik avaldus sertifikaadi saamiseks
Sertifikaat	DAS-i mõistes dokument, mis on välja antud, võimaldamaks digitaalallkirja andmist, ja milles avalik võti seotakse üheselt

Termin	Definitsioon
	füüsilise isikuga. DAS-i väliselt võib sertifikaadiomanik olla ka juriidiline isik ning sertifikaati võib kasutada ka muuks kui digitaalallkirja andmiseks.
Sertifitseerija	SK struktuuriüksus, mis väljastab ja kinnitab oma digitaalallkirjaga digitaalseid sertifikaate ja tühistusnimekirju.
Sertifitseerimispoliitika	Reeglite kogum, millega määratakse väljastatava sertifikaadi rakendusala ning rakendatavad turbenõuded.
Sertifitseerimisteenus	Sertifikaatide väljaandmise ja halduse teenus koos asjakohaste lisateenustega.
Terviklus	Andmekogumi omadus: informatsiooni pole muudetud pärast andmekogumi loomist
Turvasündmus	Sündmus, mille tagajärjeks on (või võib olla) organisatsiooni varade kadu või kahjustus, või toiming, mis on vastuolus organisatsiooni turvaprotseduuridega
Tühistusnimekiri	Kehtivuse kaotanud (kehtetuks tunnistatud, peatatud kehtivusega) sertifikaatide loetelu

11. Lühendid

Lühend	Definitsioon
CA	*(Certification Authority)* Sertifitseerija
CP	*(Certificate Policy)* Sertifitseerimispoliitika
CPS	*(Certification Practice Statement)* Sertifitseerimispõhimõtted
CRL	*(Certificate Revocation List)* Tühistusnimekiri
DAS	Eesti Vabariigi digitaalallkirja seadus
OID	*(Object Identifier)* Objektiidentifikaator, unikaalne objekti tunnuskood
PIN	*(Personal Identification Number)* Aktiveerimiskood, 4-12-kohaline numbritest koosnev salakood, mis on vajalik isikliku võtme aktiveerimiseks enne iga kasutuskorda. PIN-koodi avalikuks tulek on samaväärne isikliku võtme avalikuks tulekuga
RA	*(Registration Authority)* SK struktuuriüksus, mis tegeleb sertifikaaditaotluste vastuvõtmise, taotluse kontrolli ja/või taotluse sertifitseerijale edastamisega
RT	Riigi Teataja
SRR	Sertifitseerimise Riiklik Register
SK	Sertifitseerimisteenuse osutaja, AS Sertifitseerimiskeskus